



**System Release 7.14**

# **ASTRO<sup>®</sup> 25**

## **INTEGRATED VOICE AND DATA**

# **WINDOWS SUPPLEMENTAL CONFIGURATION**

**November 2013**

**6871025P46-A**



# Copyrights

The Motorola products described in this document may include copyrighted Motorola computer programs. Laws in the United States and other countries preserve for Motorola certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola computer programs contained in the Motorola products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola.

© 2013 Motorola Solutions, Inc. All Rights Reserved

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

## Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola contact for further information.

## Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

## European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive



The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.



# Contact Us

## Motorola Solution Support Center

The Solution Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Prior to any software reload.
- To confirm troubleshooting results and analysis prior to removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
Domestic Calls	<b>800-221-7144</b>
International Calls	<b>302-444-9800</b>

## North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Parts organization. Your first response when troubleshooting your system is to call the Motorola SSC.

For...	Phone
Phone Orders	<b>800-422-4210</b> (US and Canada Orders)  For help identifying an item or part number: select choice 3 from the menu.  <b>302-444-9842</b> (International Orders)  includes help for identifying an item or part number and for translation as needed
Fax Orders	<b>800-622-6210</b> (US and Canada Orders)

## Comments

Send questions and comments regarding user documentation to [documentation@motorolasolutions.com](mailto:documentation@motorolasolutions.com).

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola manuals. To take a short, confidential survey on Motorola Customer Documentation, go to [docsurvey.motorolasolutions.com](https://docsurvey.motorolasolutions.com) or scan the following QR code with your mobile device to access the survey.





# Document History

Version	Description	Date
6871025P46-A	Original release of the <i>Windows Supplemental Configuration</i> manual.	November 2013





# Contents

<b>Copyrights.....</b>	<b>3</b>
<b>Contact Us.....</b>	<b>5</b>
<b>Document History.....</b>	<b>7</b>
<b>List of Figures.....</b>	<b>11</b>
<b>List of Tables.....</b>	<b>13</b>
<b>List of Processes.....</b>	<b>15</b>
<b>List of Procedures.....</b>	<b>17</b>
<b>About Windows Supplemental Configuration.....</b>	<b>19</b>
What Is Covered In This Manual?.....	19
Helpful Background Information.....	19
Related Information.....	19
 <b>Chapter 1: Windows Supplemental Configuration Overview.....</b>	 <b>21</b>
Assumptions and Caveats.....	21
Windows Supplemental CD Contents.....	22
Installing Components Located on the Windows Supplemental CD .....	24
Device Name Parameters.....	25
Optional Components Located on the Windows Supplemental CD.....	26
Transferring ASTRO 25 System Files Using WinSCP.....	27
 <b>Chapter 2: Common Windows Procedures.....</b>	 <b>29</b>
Boot Order for Windows Devices (Not for Virtual Machines).....	29
Joining and Rejoining a Windows-Based Device to an Active Directory Domain with a Script.....	29
Configuration Using the ASTRO 25 System Windows Supplemental CD User Interface.....	31
Devices Supported by the ASTRO 25 System Windows Supplemental CD.....	32
Process for Using the ASTRO 25 System Windows Supplemental CD User Interface.....	33
Applying Device-Specific Settings Using the Windows Supplemental CD.....	33
Managing Local Windows Accounts Using the Windows Supplemental CD.....	35
Deploying McAfee Anti-Malware From the CSMS.....	37
CSMS – Deploying the McAfee Client Software to Anti-Malware Clients in RNI.....	37
Changing Logon Banners.....	39
Changing Logon Banners Locally.....	39
Changing Logon Banners Through a Domain Controller.....	40
Removing BAR Client and Event Logging Client Software.....	41
 <b>Chapter 3: Remote Desktop Installation and Configuration.....</b>	 <b>43</b>
Applying Remote Desktop Updates for Windows XP, Windows Server 2003, and Windows Vista.....	43
Using Windows Remote Desktop Connection.....	43
Allowing Multiple User Sessions on a Device.....	44
Changing Maximum Connections for Each Device in a Domain.....	44
Changing Maximum Connections for One Device.....	45
NetMeeting on Windows Server 2003 and Windows XP SP1-2.....	46
Starting NetMeeting on Windows Server 2003 and Windows XP SP1-2.....	46
 <b>Chapter 4: CENTRACOM Gold Elite Supplemental Configuration.....</b>	 <b>49</b>
CENTRACOM Gold Elite Operator Position Supplemental Process.....	49

ADM/CDM Server Supplemental Process.....	50
Setting Permissions for CENTRACOM Gold Folder for Windows XP and Windows Server 2003.....	50
Setting Permissions for CENTRACOM Gold Folder for Windows Vista.....	51
Setting Permissions for CENTRACOM Gold Sharing for Windows XP and Windows Server 2003.....	52
Setting Permissions for CENTRACOM Gold Sharing for Windows Vista, Windows Server 2008, and Windows 7.....	52
<b>Chapter 5: Windows Supplemental Configuration Troubleshooting.....</b>	<b>53</b>
Windows Supplemental Configuration – Types of Settings Applied.....	53

## List of Figures

Figure 1: WinSCP – Login Window .....	28
Figure 2: WinSCP – Windows Device Pane and FTP Server Pane .....	28
Figure 3: Windows Supplemental CD – Windows Security Configurations Pane .....	34
Figure 4: Windows Supplemental CD – Device Specific Settings Pane .....	35
Figure 5: Windows Supplemental CD – Windows Security Configurations Screen .....	36
Figure 6: The Deploy Agent Automation Tool Window .....	38



## List of Tables

Table 1: Windows Supplemental CD Contents .....	22
Table 2: Device Name Parameters .....	25
Table 3: Optional Components Located on the Windows Supplemental CD .....	26
Table 4: Windows Supplemental Configuration – Format of Motorola's List of Settings Automatically Applied .....	53



# List of Processes

Process for Using the ASTRO 25 System Windows Supplemental CD User Interface .....33

CENTRACOM Gold Elite Operator Position Supplemental Process ..... 49

ADM/CDM Server Supplemental Process ..... 50





## List of Procedures

Installing Components Located on the Windows Supplemental CD .....	24
Transferring ASTRO 25 System Files Using WinSCP .....	27
Joining and Rejoining a Windows-Based Device to an Active Directory Domain with a Script .....	29
Applying Device-Specific Settings Using the Windows Supplemental CD .....	33
Managing Local Windows Accounts Using the Windows Supplemental CD .....	35
CSMS – Deploying the McAfee Client Software to Anti-Malware Clients in RNI .....	37
Changing Logon Banners Locally .....	39
Changing Logon Banners Through a Domain Controller .....	40
Removing BAR Client and Event Logging Client Software .....	41
Applying Remote Desktop Updates for Windows XP, Windows Server 2003, and Windows Vista .....	43
Using Windows Remote Desktop Connection .....	43
Changing Maximum Connections for Each Device in a Domain .....	44
Changing Maximum Connections for One Device .....	45
Starting NetMeeting on Windows Server 2003 and Windows XP SP1-2 .....	46
Setting Permissions for CENTRACOM Gold Folder for Windows XP and Windows Server 2003 .....	50
Setting Permissions for CENTRACOM Gold Folder for Windows Vista .....	51
Setting Permissions for CENTRACOM Gold Sharing for Windows XP and Windows Server 2003 .....	52
Setting Permissions for CENTRACOM Gold Sharing for Windows Vista, Windows Server 2008, and Windows 7 .....	52



# About Windows Supplemental Configuration

This manual supplements the ASTRO<sup>®</sup> 25 system documentation set with additional procedures for Microsoft Windows-based devices in an ASTRO<sup>®</sup> 25 system.

This includes procedures that must be performed on all Windows-based devices in an ASTRO<sup>®</sup> 25 system, and additional procedures that are performed only for specific Windows-based devices in an ASTRO<sup>®</sup> 25 system.

## What Is Covered In This Manual?

---

This manual contains the following chapters:

- *Windows Supplemental Configuration Overview on page 21* contains assumptions and caveats for supplemental Windows configuration procedures in this manual. It also lists the contents of the ASTRO<sup>®</sup> 25 system *Windows Supplemental* CD and provides a procedure for installing specific *Windows Supplemental* CD files using a Windows Install Framework script. It also provides an introduction to using the WinSCP utility for file transfers.
- *Common Windows Procedures on page 29* contains common supplemental configuration procedures for Windows-based devices in ASTRO<sup>®</sup> 25 systems.
- *Remote Desktop Installation and Configuration on page 43* provides remote desktop configuration information and procedures for Windows-based devices in ASTRO<sup>®</sup> 25 systems.
- *CENTRACOM Gold Elite Supplemental Configuration on page 49* contains procedures related to the Gold Elite Operator and Server.
- *Windows Supplemental Configuration Troubleshooting on page 53* provides a way to determine types of ASTRO<sup>®</sup> 25 system supplemental configuration settings applied to specific Windows-based devices.

## Helpful Background Information

---

Motorola offers various courses designed to assist in learning about the system.

For information, go to <http://www.motorolasolutions.com/training>.

## Related Information

---

Refer to the following documents for associated information about the radio system:

Related Information	Purpose
<i>Standards and Guidelines for Communication Sites</i> (6881089E50)	Provides standards and guidelines that should be followed when setting up a Motorola communications site. Also known as R56 manual.  This manual may be purchased on CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
<i>System Documentation Overview</i>	For an overview of the ASTRO <sup>®</sup> 25 system documentation, open the graphical user interface for the ASTRO <sup>®</sup> 25 system documentation set and select the <b>System Documentation Overview</b> link. This opens a file that includes:

*Table continued...*

Related Information	Purpose
	<ul style="list-style-type: none"><li>• ASTRO<sup>®</sup> 25 system release documentation descriptions</li><li>• ASTRO<sup>®</sup> 25 system diagrams</li><li>• ASTRO<sup>®</sup> 25 system glossary</li></ul> <p>For an additional overview of the system, review the architecture and descriptive information in the manuals that apply to your system configuration.</p>
<i>Virtual Management Server Software</i>	For detailed information on the VMware vSphere Client.

# Chapter 1

## Windows Supplemental Configuration Overview

This chapter contains assumptions and caveats for supplemental Windows configuration procedures in this manual. It also lists the contents of the *Windows Supplemental CD*.

### Assumptions and Caveats

---

This document assumes the following:

- The operating system has been installed and correctly configured.
- All the correct operating system patches have been applied and correctly configured.
- All necessary domains have been **Trusted** according to the installation requirements.
- All the product applications have been installed and correctly configured.

If these assumptions are not met, do not proceed with the procedures in this document.



#### **Important:**

- To successfully complete the procedures, you must perform all the procedures when logged in as a valid domain or local Windows administrator (except where otherwise stated).
- Depending on the device configuration, when you perform administrative tasks on the Microsoft Windows Vista operating system, Windows Server 2008 operating system, or on the Windows 7 operating system, a User Account Control (UAC) dialog box might prompt you to click **Continue** or **Allow**, or it may prompt you to provide domain or local Windows administrator credentials.
- After applying procedures, the Windows **Autorun** (also known as Autoplay) feature is turned off, which means its functionality is no longer accessible. For example, CDs do not automatically start when inserted in the drive, nor is the name of the CD automatically refreshed in Windows Explorer.
- After procedures are applied, passwords for existing user accounts will continue to work. However, password complexity requirements will be enforced when the existing passwords are changed. The password requires at least one upper case letter and one lower case letter, and at least one number and one special character. The password length requirement is 14 characters for Windows-based devices.
- Applying procedures to any device/application other than what is explicitly mentioned in this manual is not recommended. Doing so may require a reinstallation of the operating system.
- Removing a Windows-based device from a domain, when the Domain Controller is not available, may result in a permanently undesirable state that will require a reinstallation of the operating system. Always make sure that the Domain Controller is operating and authenticate the removal from the domain at the Domain Controller.

## Windows Supplemental CD Contents

**Table 1: Windows Supplemental CD Contents**




Contents of CD	For instructions, see:
Motorola Windows Security Configurations	<a href="#">Common Windows Procedures on page 29</a>
Remote Desktop:	<a href="#">Remote Desktop Installation and Configuration on page 43</a>
<ul style="list-style-type: none"> <li>• Updates</li> <li>• Script to aid remote access through NetMeeting</li> </ul>	
Motorola Windows Backup and Restore (BAR) Client for ASTRO® 25 system BAR services	<ul style="list-style-type: none"> <li>• For installation instructions, see <a href="#">Installing Components Located on the Windows Supplemental CD on page 24</a>.</li> <li>• For detailed information, see the <i>Backup and Restore Services</i> manual.</li> </ul>
Motorola Windows Event Logging Client for ASTRO® 25 system Centralized Event Logging service	<ul style="list-style-type: none"> <li>• For installation instructions, see <a href="#">Installing Components Located on the Windows Supplemental CD on page 24</a>.</li> <li>• For detailed information, see the <i>Centralized Event Logging</i> manual.</li> </ul>
PuTTY	<p>PuTTY is the utility that is certified for initiating interactive sessions in Secure SHell (SSH) or other protocols.</p> <p>The utility and the <i>PuTTY</i> User Manual are available by navigating to the list of programs on your computer, and selecting <b>Motorola</b> → <b>Motorola PuTTY</b>. The .msi package is customized by Motorola.</p> <ul style="list-style-type: none"> <li>• For installation instructions, see <a href="#">Installing Components Located on the Windows Supplemental CD on page 24</a>.</li> <li>• For detailed information, see the <i>Securing Protocols with SSH</i> manual.</li> </ul>
WinSCP	<ul style="list-style-type: none"> <li>• See <a href="#">Transferring ASTRO 25 System Files Using WinSCP on page 27</a>.</li> <li>• For installation instructions, see <a href="#">Installing Components Located on the Windows Supplemental CD on page 24</a>.</li> <li>• For detailed information, see <a href="http://www.winscp.net">www.winscp.net</a>.</li> </ul>
OpenSSL	<ul style="list-style-type: none"> <li>• For installation instructions, see <a href="#">Installing Components Located on the Windows Supplemental CD on page 24</a>.</li> <li>• For detailed information, see <a href="http://www.openssl.org">www.openssl.org</a>.</li> </ul>
Motorola Certificate Generation and Deployment (CGD)	For installation instructions and prerequisites, see <a href="#">Installing Components Located on the Windows Supplemental CD on page 24</a> .
Motorola CA Certs (MOT_CACerts)	<p>An .msi package installing public root certificates for SSC and ASTRO® 25 systems. These are public certificates required by client devices to authenticate with different web services which are using Motorola certificates.</p> <p> <b>Note:</b> This package is <b>not</b> supported on Windows XP.</p> <p>For installation instructions and prerequisites, see <a href="#">Installing Components Located on the Windows Supplemental CD on page 24</a>.</p>

Table continued...

Contents of CD	For instructions, see:
<p>SNMP Common Agent configuration file folder (only use the files in this folder if instructed to do so in the ASTRO® 25 system manual for the Windows-based device or in the <i>SNMPv3</i> manual):</p> <p>\Motorola Common Agent\</p>	<p>SNMP-related procedures for individual devices are located in the ASTRO® 25 system manual for that device.</p> <p>For general information about SNMPv3 in ASTRO® 25 systems, see the <i>SNMPv3</i> manual.</p> <p>For detailed information on how to install the Common Agent, refer to the <i>SNMPv3</i> manual.</p>
<p>SNMPv3 passphrase configuration utility (SNMPv3 Credential GUI)</p>	<p>Used by SNMP Common Agent to reset credentials. For detailed information, see the <i>SNMPv3</i> manual.</p>
<p>Group Policy Objects</p> <p>located under:</p> <p>\ActiveDirectory\</p> <p>Scripts related to Active Directory and DNS, including script for Windows devices to join the domain are</p> <p>located under:</p> <p>\Motorola JoinADomain</p>	<p>For detailed information, see the <i>Authentication Services</i> manual.</p>
<p>Other common software:</p> <ul style="list-style-type: none"> <li>• Adobe Reader</li> <li>• Sun Java Runtime Environment (JRE)</li> </ul>	<p>Documentation provided by the company that produced the software.</p> <p>You can also load Adobe Reader from the ASTRO® 25 system documentation media.</p> <p>If you install Adobe Reader, see the <i>Readme.txt</i> file on the latest <i>MOTOPATCH for Windows 3PP CD</i> and install the patch if required by your organization.</p> <p>For detailed information, refer to <i>Installing Components Located on the Windows Supplemental CD on page 24</i>.</p>
<p>Motorola Embedded Password Management</p> <p> <b>Note:</b> Embedded Password Management is only for supported devices, as indicated in the “Appendix C” of the <i>Authentication Services</i> manual.</p>	<p>For detailed information, see the <i>Authentication Services</i> manual.</p> <p>For installation instructions and prerequisites, see <i>Installing Components Located on the Windows Supplemental CD on page 24</i>.</p>
<p>Motorola AAA API Package</p> <p> <b>Note:</b> This package is for CAM server and NM Client only.</p>	<p>For detailed information, see the <i>Authentication Services</i> manual, the <i>MKM 7000 Console Alias Manager</i> manual, and the <i>Private Network Management Client</i> manual.</p> <p>For installation instructions and prerequisites, see <i>Installing Components Located on the Windows Supplemental CD on page 24</i>.</p>
<p>7-Zip</p>	<p>Archiving software that can be used to compress and uncompress files.</p>

## Installing Components Located on the Windows Supplemental CD

**Prerequisites:** Obtain the *Windows Supplemental CD*.

**When and where to use:** This procedure describes the scenarios for using the Windows Install Framework application and can be used to automatically and simultaneously install all the required common software components from the *Windows Supplemental CD*, for one of the devices listed in [Device Name Parameters on page 25](#), as well as any necessary cohabitation devices and optional components listed in [Optional Components Located on the Windows Supplemental CD on page 26](#).

For example, required common components for the NM Client are: PuTTY, OpenSSL, CGD, MOT\_CACerts, Embedded Password Management, Acrobat Reader, JRE, and AAA API. Using the following procedure, you can install them all without the necessity to reinsert the *Windows Supplemental CD*.

Similarly, AuC Client can be installed as a device cohabitating on the same operating system as the NM Client and Centralized Event Logging client and Backup and Restore Client as optional components of the NM Client.



**Important:** Installation of components located on the *Windows Supplemental CD* is supported only in the pre-defined location and cannot be changed by the user.

### Procedure:

- 1 If you are installing to a Windows-based device that is a virtual machine, connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental CD* for this procedure.

See the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.

- 2 Log on to a Windows-based device with a local Windows administrator account.



**Note:** The account name set up by Motorola for Windows Vista-based and Windows 7-based devices is “secmoto”. For Windows Server 2008 and Windows Server 2003-based devices the account will be “administrator” until you complete the following and the account becomes “motosec”: [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#) or [Joining and Rejoining a Windows-Based Device to an Active Directory Domain with a Script on page 29](#).

- 3 Insert the *Windows Supplemental CD* into the CD/DVD drive.
- 4 Open the Command Prompt.

**Step result:** The Command Prompt appears.

- 5 Navigate to the \wif directory on the CD/DVD drive.
- 6 Depending on the component you need, execute the following command (consisting of one, two, or three parameters, separated with a space):

```
WindowsInstallFramework.exe /e /i <device name>.xml <cohab device name>.xml
<optional component>.xml
```

Where:

- **<device name>** is only one of the parameters listed in [Device Name Parameters on page 25](#)



**Note:** To see the list of common components to be installed for a device in [Device Name Parameters on page 25](#), from the Supplemental CD/wif location, open the xml file for a device in Notepad and, within it, search for <AppName>.

- **<cohab device name>** is the name of a device cohabitating on the same operating system, for example, AuC Client can cohabitate with NM Client
- **<optional component>** is one or more of the components, separated with a space, listed in [Optional Components Located on the Windows Supplemental CD on page 26](#).

### Step example:

```
WindowsInstallFramework.exe /e /i NETWORK_MANAGEMENT_CLIENT.xml
AUTHENTICATION_CLIENT.xml "Motorola Windows Bar Client.xml" "Motorola
Windows Logging Client.xml"
```





**Note:** For Windows 7, insert quotes around filenames that contain spaces.



**Note:** If the **User Account Control** dialog box appears, click **Continue**, or type the administrator password for the account displayed then click **Yes**, depending on the prompt you see.

**Step result:** An installation finished message appears.

7 Click **OK**.

8 If you installed these applications to a virtual machine and have no additional operations to perform for this virtual machine from the DVD drive, it is recommended that you disconnect the virtual machine from the DVD drive. For instructions, see the *Virtual Management Server Software* manual.

#### Post requisites:



**Note:** Before using any of the components that have been installed during this procedure, it is recommended that you reboot the device.



#### Important:

If any of the components is missed during an installation, it can be additionally installed after performing this procedure. For example, to individually install one of the missing optional components, execute the following command:

```
WindowsInstallFramework.exe /e /i <optional component>.xml
```

## Device Name Parameters

**Table 2: Device Name Parameters**

Device	<device name>.xml
Authentication Center (AuC) Client	AUTHENTICATION_CLIENT.xml
Authentication Center (AuC) Server	AUTHENTICATION_SERVER.xml
MOSCAD NFM Graphical Master Computer (GMC)	GRAPHICAL_MASTER_COMPUTERS.xml
MOSCAD NFM Graphical Workstation (GWS)	GRAPHICAL_WORKSTATION.xml
FSA4000 Alerting LAN Computer (ALC)	ALERTING_LAN_COMPUTERS.xml
FSA4000 Alerting Master Computer (AMC)	ALERTING_MASTER_COMPUTERS.xml
NM Client	NETWORK_MANAGEMENT_CLIENT.xml
MKM 7000 Console Alias Manager (CAM) server	CAM_SERVER.xml
MCC 7500 Dispatch Console hosting Radio Control Manager (RCM)	RCM.xml
Key Management Facility (KMF) Server	KMF_SERVER.xml
Key Management Facility (KMF) Client	KMF_CLIENT.xml
Core Security Management Server (CSMS)	CSMS.xml



## Optional Components Located on the Windows Supplemental CD




**Note:** Installation of files located on the *Windows Supplemental* CD is supported only in the pre-defined location and cannot be changed by the user.

Many of these files are part of initial installation. For example, OpenSSL and Embedded Password Management are part of initial installation on supported ASTRO<sup>®</sup> 25 system devices, such as NM Client. However, there may be a need for installing optional software separately (for example, Centralized Event Logging client and Backup and Restore Client for the NM Client). The following table lists all components located on the *Windows Supplemental* CD which, if needed, can be installed as optional.

**Table 3: Optional Components Located on the Windows Supplemental CD**

Component Name	Component Description	Component Filename
<b>Backup and Restore (BAR) client application</b>	For Windows-based devices that use the full implementation of the ASTRO <sup>®</sup> 25 system BAR service (for feature details, see the <i>Backup and Restore Services</i> manual).	Motorola Windows Bar Client.xml
<b>Event Logging client application</b>	For Windows-based devices that use the ASTRO <sup>®</sup> 25 system Centralized Event Logging service (for feature details, see the <i>Centralized Event Logging</i> manual).	Motorola Windows Logging Client.xml
	 <b>Important:</b> You should install the BAR client and Logging client at the point indicated in the overall installation/configuration process in the manual for a Windows-based device in an ASTRO <sup>®</sup> 25 system.	
<b>PuTTY version customized by Motorola</b>	Can be used to initiate secure sessions with other devices that support secure protocols (see the <i>Securing Protocols with SSH</i> manual).	Motorola PuTTY.xml
<b>WinSCP</b>	Can be used to drag and drop files between a Windows-based device and an FTP server (see <a href="#">Transferring ASTRO 25 System Files Using WinSCP on page 27</a> ).	Motorola WinSCP.xml
<b>OpenSSL</b>	A toolkit implementing the Secure Sockets Layer, Transport Layer Security, and general purpose cryptography library.	Motorola OpenSSL.xml
	 <b>Note:</b> Make sure OpenSSL is installed before the CGD tool.	

*Table continued...*

Component Name	Component Description	Component Filename
<b>Motorola Certificate Generation and Deployment (CGD) tool</b>	Creates and distributes Motorola default certificates for target windows devices to authenticate with the installed Trusted Root Certificate.	Motorola Certificate Generation Deployment Tool.xml
<b>Adobe Reader</b>	Application used to view files in the .pdf format.	Motorola ASTRO Adobe Reader.xml
<b>JRE 6 (Java Runtime Environment)</b>	Allows your system to run Java applications and websites.	Motorola ASTRO Java 6.xml
<b>JRE 7 (Java Runtime Environment)</b>	Allows your system to run Java applications and websites.	Motorola ASTRO Java Family.xml
<b>Motorola Embedded Password Management</b>	Used to change embedded account passwords on supported devices (see “Appendix C” of the <i>Authentication Services</i> manual.	Motorola Password Vault.xml
<b>Motorola AAA API</b>	The AAA API provides a consistent interface to authenticate and retrieve authorization information from Active Directory. It also provides a mechanism for authenticating a user if Kerberos is unavailable.	Motorola AAA API.xml
<b>Remote Desktop Update</b>	Remote Desktop Update for Windows XP, Windows Server 2003, and Windows Vista.	remote_desktop_updates.xml
<b>Motorola CA Certs</b>	An .msi package installing public root certificates for SSC and ASTRO® 25 systems. These are public certificates required by client devices to authenticate with different web services which are using Motorola certificates.	Motorola MOT_CACerts.xml
 <b>Note:</b> This package does <b>not</b> support Windows XP.		

## Transferring ASTRO 25 System Files Using WinSCP

**Prerequisites:** To use WinSCP for transferring files in an ASTRO® 25 system:

- Confirm that there is available hard drive space on the device where you plan to transfer the files.
- Confirm that file transfer is permitted between the FTP server and the device where you plan to transfer the BAR archive files. If so, confirm which file transfer protocol is required by your organization.

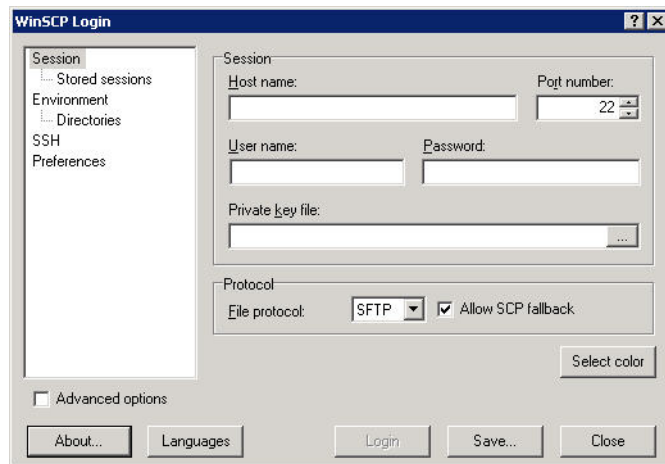
### When and where to use:

The open source WinSCP utility available on the ASTRO® 25 system *Windows Supplemental* CD can be used to transfer files, using a drag-and-drop GUI, to and from an FTP server device.

Detailed instructions for using WinSCP are available at <http://winscp.net>.

### Procedure:

- 1 To launch **WinSCP**, click **Start** → **Programs** → **WinSCP**.

2 On the **WinSCP Login** window:**Figure 1: WinSCP – Login Window**

- a) Enter the hostname of the FTP server.
  - b) Enter the user name and password of an Active Directory account that is a member of the “bkupadm” user group.
  - c) Select the appropriate file transfer protocol, depending on your organization's policies.
  - d) Click **Login**.
- 3 In the WinSCP navigation pane for the FTP server:

**Figure 2: WinSCP – Windows Device Pane and FTP Server Pane**

- a) Navigate from your user account home directory to the directory with the files you want to transfer.
- b) Drag and drop files from the FTP server navigation pane to the Windows navigation pane in WinSCP.

# Chapter 2

## Common Windows Procedures

This chapter provides common supplemental procedures for Windows-based devices in an ASTRO<sup>®</sup> 25 system.

### Boot Order for Windows Devices (Not for Virtual Machines)

---

For all Windows-based devices in an ASTRO<sup>®</sup> 25 system that are **not** implemented as virtual machines, ensure that the boot order is set as follows:

- 1 Internal hard drives
- 2 Internal optical drives
- 3 External hard drives
- 4 External USB devices

The boot order and configuration for a PC is found in the PC's BIOS. Refer to the PC manufacturer's documentation for instructions on how to set the boot order correctly.



**Note:** The boot order needs to be set once and then verified each time the operating system is installed. In an ASTRO<sup>®</sup> 25 system, the ESXi-based host for virtual machines does not support the use of USB drives.

### Joining and Rejoining a Windows-Based Device to an Active Directory Domain with a Script

---

#### Prerequisites:

Obtain from your system administrator the Organizational Unit for this Windows-based device, as well as the user name and password for the account that is used to join this Windows-based device to the Active Directory domain.

For a list of Windows-based devices, see “Active Directory Client Devices and Applications” in the *Authentication Services* manual.

If the Windows-based device is a virtual machine, before performing this procedure, make sure that the virtual machine is connected to the DVD drive where you will insert the software media. For information about connecting DVD drives to virtual machines in ASTRO<sup>®</sup> 25 systems, see the *Virtual Management Server Software* manual.

#### When and where to use:

The join domain operation automatically unjoins the device from any domain it may have been previously joined to.

The script for joining a Windows client to the domain automatically configures NTP, DNS and OU for that client.

If the device has problems joining the domain:

- Ensure the time is synchronized between the client and the AD/DNS.
- Verify the DNS server in the TCP/IP properties of the Network Interface Card (NIC) is set to the correct DNS Server IP.

- Verify the Network Connectivity is up and domain controllers are reachable.



**Important:**

While rejoining a Windows-based device to an Active Directory Domain, do **not** use this script to move the Windows-based device from an Organization Unit to another Organization Unit.

**Procedure:**

- 1 If a Windows logon dialog box appears, enter the credentials for a Windows user account that is maintained locally on this Windows-based device.

If you are logging on with a local account, and you need to perform operations requiring Windows administrator privileges, log on with a local Windows administrator account.

The account names set up by Motorola include “secmoto” for Windows Vista and Windows 7-based devices, and “motosec” for all other Windows OS devices.

**Step result:** The administrator's desktop appears.

- 2 Insert the *Windows Supplemental* CD in the drive.
- 3 Perform one of the following actions, depending on the Windows OS version:
  - If the OS of the device is Windows XP or Windows Server 2003, copy the `joinADomain_2003_XP.exe` and `joinADDomain.hta` files from the Motorola `JoinADomain\Windows2003_XP` folder on the *Windows Supplemental* CD to the `C:\windows\temp` directory on the hard drive.
  - If the OS of the device is Windows Vista, Windows 7, or Windows Server 2008, navigate to the Motorola `JoinADomain\OtherWindowsOS` folder on the *Windows Supplemental* CD.
- 4 Perform one of the following actions, depending on the Windows OS version:
  - If the OS of the device is Windows XP or Windows Server 2003, in the `C:\windows\temp` folder, double-click `joinADomain_2003_XP.exe`.
  - If the OS of the device is Windows Vista, Windows 7, or Windows Server 2008, in the Motorola `JoinADomain\OtherWindowsOS` folder, double-click `JoinADomain.exe`.

**Step result:** The **Join Active Directory Domain** window appears.



**Note:** If an error message appears reporting that the application could not locate the AD domain, enter the **<AD Domain Name>** manually in the **AD Domain Name** field. For details, see “User Input Requirements – Domain Controller Configuration” in the *Authentication Services* manual.

If a command prompt opens along with the Join Active Directory Domain window, do not close the command prompt, as it will go away when the Join AD Domain window is closed.

If a **User Account Control** dialog box appears, click **Allow**, **Yes**, or **Continue**, depending on the prompt, then fill in the required fields for the account displayed and click **Yes**.

- 5 When prompted, log on to the domain controller using your Active Directory account that is a member of the Domain Admins group, or using the local Windows administrator account.  
The default domain administrator account is “motosec”.



**Note:** If the **Organizational Unit** field does not update automatically, tab out of the password or **AD Domain Name** field or click the **Username** field.

**Step result:** The **Organizational Unit** field is updated with the information entered.

- 6 Select the correct **Organizational Unit** for the Windows-based device from the OU drop-down list.

**Step example:**

- The OU for Network Management Clients is **Network Management Clients**
- The OU for Core Security Management Server is **Security Management Servers**
- The OU for a MOSCAD Network Fault Management (NFM) Graphical Master Computer (GMC) is **Graphical Master Computers**

- The OU for a MOSCAD NFM Graphical Workstation (GWS) is **Graphical Workstations**

**7 For cohabited applications:** select the OU of the primary device on which the cohabited application is placed.  
**Step example:** When joining a Windows 7 Authentication Center (AuC) Client cohabited with Windows 7 Network Management Clients to the domain, from the drop-down list, select **Windows 7 Network Management Clients OU**.

**8 Click Join.**

**For Windows 7:** if a message window appears stating that Windows Firewall has blocked some features of the program, click **Allow Access**.

**Step result:** In case of Windows XP and Windows Server 2003-based devices, a message states that the Windows-based device has been successfully joined to the AD domain. In case of Windows Vista, Windows 7, and Windows Server 2008-based devices, a message states that the Windows-based device has been successfully joined to AD in the INFO text area. A reboot window appears.



**Note:** If an error message appears, repeat the procedure. If the error persists, contact the Motorola Solution Support Center (SSC).

**9** Perform one of the following actions, depending on the Windows OS version:

- If the OS of the device is Windows XP or Windows Server 2003, click **Reboot** to restart the device.
- If the OS of the device is Windows Vista, Windows 7, or Windows Server 2008, click **Yes** to restart the device.

**Step result:** The client reboots.

#### Post requisites:



**Note:** After a device joins the domain, its applications that have Role Based Access Control in Active Directory may not be usable by the local Windows administrator or the domain administrator if that user account is not a member of the group associated with the application for that device.

In some cases, the administrator can access the application by entering its executable path and filename at the elevated Windows command line. The path and filename can be seen in the properties for the application shortcut on the desktop or **Start** menu. For information how to run the elevated Windows command line, see “Starting the Windows Command Line as Administrator” in the *Authentication Services* manual.



**Note:** For Voice Card and Crypto Card-based consoles, after joining the device to the domain and rebooting the console, run GPUUpdate or force it from a Windows command prompt.

## Configuration Using the ASTRO 25 System Windows Supplemental CD User Interface

---

*Applying Device-Specific Settings Using the Windows Supplemental CD on page 33* is not mandatory for Windows-based devices that are joined to the ASTRO® 25 domain, except for the following devices, or in cases where your organization has requested that local security be applied to all devices:

- MGE
- AuC Server
- AuC Client

*Managing Local Windows Accounts Using the Windows Supplemental CD on page 35* is not required but can optionally be used to change passwords of specific local Windows accounts.





**Important:** Perform these procedures on devices that have local security applied whenever any software (including the operating system) is installed or upgraded on any Windows-based device in an ASTRO® 25 system.

After you perform [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#), if your organization requires its own modifications to local Group Policy User Configuration settings on this Windows-based device, your organization's settings will need to be reconfigured (for example, modifying the secure Screen Saver settings). Refer to Microsoft documentation for details about how to modify local Group Policy User Configuration settings using `gpedit.msc`.

## Devices Supported by the ASTRO 25 System Windows Supplemental CD

Windows-based devices are supported by the ASTRO® 25 system *Windows Supplemental CD*. Various combinations of these devices are also supported for cohabitation on the same physical device. When you perform [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#), the drop-down list on the **Device Specific Settings** window provides a way for you to select from a list that includes the devices below, and also the supported cohabitation combinations of devices.

The following devices are supported by the ASTRO® 25 system *Windows Supplemental CD*:

- Authentication Center (AuC) Client
- Authentication Center (AuC) Server
- CENTRACOM ADM/CDM Server
- CENTRACOM Gold Elite Dispatch Console
- Configuration Manager\*
- Core Security Management Server (CSMS)
- Data Collection Device (DCD) for Motorola use only
- FSA4000 Alerting LAN Computer (ALC)
- FSA4000 Alerting Master Computer (AMC)
- InfoVista Server
- IP PBX Server (Telephony server)
- KMF Client
- KMF Server
- MCC 7100 IP Dispatch Console
- MCC 7500 Dispatch Console and AIS
- MCN (CTI) Server 8000 (Remote Comparator Display Software for Motorola IP Comparators)
- MCN (CTI) Client
- MKM 7000 Console Alias Manager (CAM) server
- MOSCAD NFM Graphical Master Computer (GMC)
- MOSCAD NFM Graphical Workstation (GWS)
- Motorola Gold Elite Gateway (MGEG)
- Logging Recorder
- Replay Station
- NM Client
- PRX 7000 Console Proxy

\* [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#) applies for the Configuration Manager. However, if the text string Configuration Manager does **not** appear in the .txt file located at \Motorola Windows Supplemental Fullconfig\bin\ or \Motorola Windows Supplemental Transconfig\bin\, depending on your organization's policies, on the *Windows Supplemental CD* provided with your ASTRO® 25 system, then you do not need to perform [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#).



**Note:** If a device or application is not listed in this section, refer to the product's documentation for supplemental configuration instructions.



## Process for Using the ASTRO 25 System Windows Supplemental CD User Interface

**Prerequisites:** Obtain the *Windows Supplemental* CD provided by Motorola for your system. Except for the following devices, or in cases where your organization has requested that local security be applied to all devices, the following process is **not** mandatory for Windows-based devices that are joined to the ASTRO® 25 domain:

- MGE
- AuC Server
- AuC Client

**When and where to use:** When using the *Windows Supplemental* CD user interface, this process must be completed in the order shown.

### Process:

- 1 If you are applying this process to a Windows-based device that is implemented as a virtual machine, you first need to connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental* CD. Refer to the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.
- 2 Perform [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#).



**Important:** The Device-Specific Settings procedure changes password criteria for the Windows accounts. For Windows Server 2003 and Windows Server 2008 devices, it changes the local Windows administrator account name to “motosec”.

- 3 Optionally, perform [Managing Local Windows Accounts Using the Windows Supplemental CD on page 35](#) to set up new passwords for the applicable Windows accounts.
- 4 Reboot the device.
- 5 If you applied settings to a Windows-based device that is a virtual machine and have no additional operations to perform for this virtual machine from the DVD drive, it is recommended that you disconnect the virtual machine from the DVD drive. For instructions, see the *Virtual Management Server Software* manual.

## Applying Device-Specific Settings Using the Windows Supplemental CD

**Prerequisites:** See [Windows Supplemental Configuration Troubleshooting on page 53](#) for viewing summary information about the types of settings applied.

**When and where to use:** Perform this procedure to apply supplemental configuration settings for a specific Windows-based device in an ASTRO® 25 system.



**Important:** Perform this procedure whenever any software (including the operating system) is installed or upgraded on any Windows-based device in an ASTRO® 25 system.

Except for the following devices, or in cases where your organization has requested that local security be applied to all devices, the following procedure is **not** mandatory for Windows-based devices that are joined to the ASTRO® 25 domain:

- MGE
- AuC Server
- AuC Client

### Procedure:

- 1 Log in to the Windows-based device using a valid domain account or local Windows “administrator” account.
- 2 Insert the *Windows Supplemental* CD into the DVD drive.



**Note:** If you are applying this procedure to a Windows-based device that is implemented as a virtual machine, you first need to connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental* CD. Refer to the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.

3 Depending on your organization's policies, navigate to one of the following folders:

- Motorola Windows Supplemental Fullconfig\bin\
- Motorola Windows Supplemental Transconfig\bin\

4 Double-click **Windows\_Supplemental\_GUI.exe**.



**Note:** If the **User Account Control** dialog box appears, click **Continue**, or type the administrator password for the account displayed then click **Yes**, depending on the prompt you see.



**Important:** Wait until the *Windows Supplemental* CD window appears. This may take up to 3 minutes.

**Step result:** The Command Prompt quickly opens and closes, then **The Windows Supplemental CD** window appears.

5 Click **Windows Security Configurations**.

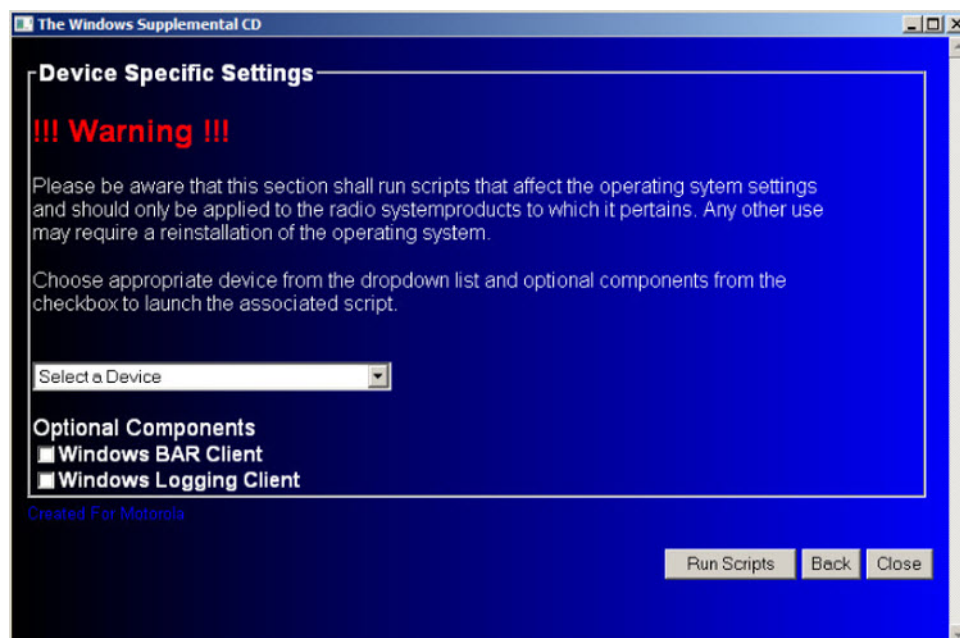
6 In the **Windows Security Configurations** pane, click **Device Specific Settings**.

**Figure 3: Windows Supplemental CD – Windows Security Configurations Pane**



7 In the **Device Specific Settings** pane, from the drop-down list, select the appropriate device supported by the operating system on the Windows-based device you are currently using.

Figure 4: Windows Supplemental CD – Device Specific Settings Pane



**Note:** Be sure to review the entire list before selecting the device. The list includes various cohabitation options.

8 Select the check box for either one or both optional components that apply to this device:

- **Windows BAR Client**
- **Windows Logging Client**

If you are unsure which options apply to this device, contact your system administrator and refer to:

- The Windows-based Event Logging client procedures in the *Centralized Event Logging* manual
- The Windows-based BAR client procedures in the *Backup and Restore Services* manual

9 Click **Run Scripts**.

10 On the prompt, click **OK**.

**Step result:** The command prompt window displays messages as all the device-specific settings for this device type are applied. Then a list of all the settings applied displays on the screen.

11 Click **OK**.

12 Leave the *Windows Supplemental CD* in the drive of the Windows-based device and do **not** close the *Windows Supplemental CD* user interface, if you want to proceed to [Managing Local Windows Accounts Using the Windows Supplemental CD on page 35](#).

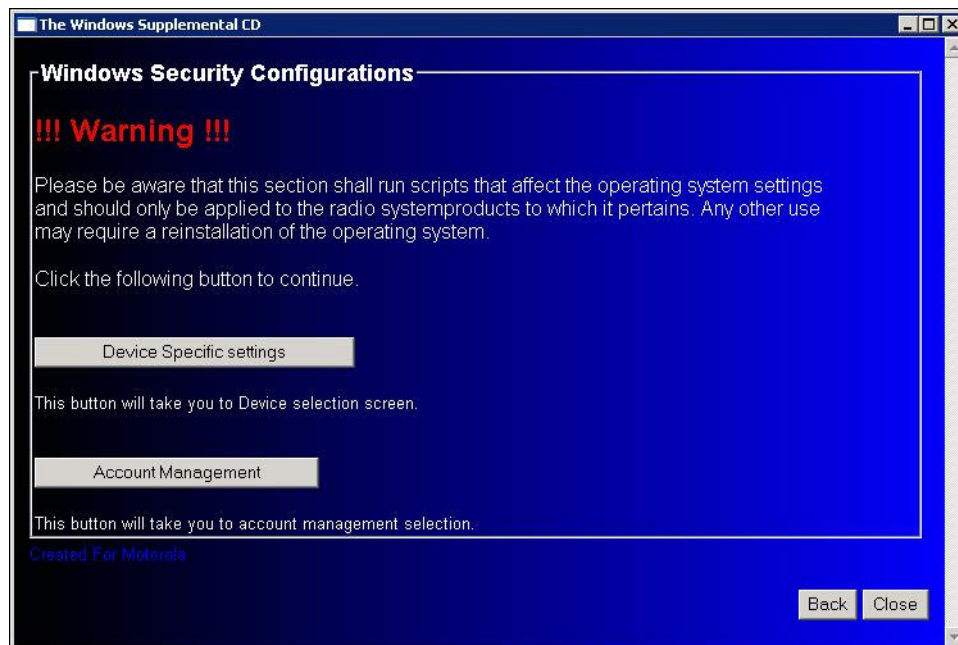
## Managing Local Windows Accounts Using the Windows Supplemental CD

**Prerequisites:** Obtain the *Windows Supplemental CD*.

**When and where to use:** This procedure is not required but can optionally be used to change passwords of specific local Windows accounts whenever any software (including the operating system) is installed or upgraded on an ASTRO® 25 system Windows-based device.

### Procedure:

1 Click **Windows Security Configurations** on the left side of the *Windows Supplemental CD* screen.

**Figure 5: Windows Supplemental CD – Windows Security Configurations Screen**

**Step result:** The **Windows Security Configurations** screen appears.

- 2 Click **Account Management** on the left side of the screen.

**Step result:** The Account Management Settings window appears.

- 3 Click **Administrator Account**.
- 4 At the prompt, enter the password for the administrator account.
- 5 At the prompt, re-enter the password.



**Note:** Before pressing a key, ensure that the preceding steps were successful by referring to the message in the command prompt.

- 6 Press any key.

**Step result:** The command prompt window closes and the following message appears:

```
Account management scripted has completed,
follow instructions from command line
```

- 7 Click **OK**.
- 8 On the Account Management Settings window, click **Guest Account** and repeat [step 4](#) through [step 7](#).



**Note:** For Windows Vista-based devices, Windows 7-based devices, and Windows Server 2008 devices, skip to [step 10](#). (Do **not** click **Support Account**.)

- 9 For Windows Server 2003-based devices, click **Support Account**, and repeat [step 4](#) through [step 7](#).



**Note:**

**Support Account** is not applicable to Windows Server 2008-based devices, Windows Vista, or Windows 7-based devices.

If you accidentally click **Support Account** for a Windows Vista-based device, Windows 7-based device, or a Windows Server 2008 device, a message states that the user name could not be found. Ignore instructions to rerun the script, and press any key to return to the *Windows Supplemental CD* window.

- 10 Click **Close** to exit the *Windows Supplemental CD* window.

11 Reboot the device.

**Step result:** Security settings take effect.

## Deploying McAfee Anti-Malware From the CSMS

---

Deployment of McAfee Anti-Malware from the CSMS is required in order to configure each anti-malware client with the unique hostname for the CSMS, which hosts the McAfee Anti-Malware server.

For more information, see the *Core Security Management Server* manual.

## CSMS – Deploying the McAfee Client Software to Anti-Malware Clients in RNI

Deploy the McAfee ePO Client Software by using the Deployment Automation tool developed by Motorola. This tool provides the option of pushing agent and its component to a single IP or to a list of IP addresses that are passed as text file.



### Important:

Before you deploy the McAfee VirusScan Enterprise product on the device, refer to the product manual to confirm that McAfee VirusScan Enterprise is supported by the given device or application. Deploying McAfee to a non-supported product may have unintended consequences.

### Prerequisites:

Join:

- The Active Directory domain for any RNI Windows device to which the McAfee client software will be deployed.
- Core Security Management Server (CSMS) to the Active Directory domain.

Ensure that CSMS has access to the RNI Windows device on the network.

McAfee Client Software can be pushed only to a single operating system at a time. For example, when you provide a list of IP addresses, you can only provide IP addresses for Windows devices or RHEL5 devices or RHEL6 devices. You cannot have a mix of Windows, RHEL5 and RHEL6 IPs passed as an input to the deployment tool. Therefore:

- Obtain from your system administrator the IP address of each Windows, Linux RHEL5, and Linux RHEL6 devices to which the McAfee ePO client software will be deployed.
- Create separate `.txt` files for each operating system.

Each `.txt` file contains only a single IP address on each line and in the standard AAA.BBB.CCC.DDD format.



**Note:** Push McAfee Client Software to devices which are multi-homed (Multiple NICs/IP addresses) using the primary IP address assigned to the device.

### When and where to use:

Deploy the McAfee client software from a CSMS to one or more ASTRO<sup>®</sup> 25 system radio network infrastructure (RNI) Windows, Linux RHEL5, and Linux RHEL6 devices in an ASTRO<sup>®</sup> 25 system.



**Important:** When deploying VSE to the Firewall Management Server, the Deployment Automation tool and Agent Report might show a failure for the VSE installation even though VSE is installed on the Firewall Management Server. Check the McAfee ePO console to determine whether VSE is installed on Firewall Management Server.

### Procedure:

- 1 Log on to the CSMS using a domain account belonging to the `secadm` or domain admin group.
- 2 In the desktop that appears, double-click the **Deploy\_McAfee\_Agent** icon.



**Note:** If the **User Access Control** dialog window appears, perform one of the following actions:

- Click **Continue**.
- Type the administrator password for the account that appears. Click **Yes**.

- 3 In the **OS Type** section from the **Deploy Agent Automation Tool** window that appears, select the appropriate OS type to indicate the Client OS that you want to push the software to.

**Figure 6: The Deploy Agent Automation Tool Window**

- 4 Select the **Agent** and **VSE** check boxes.



**Note:** If you want to install VirusScan Enterprise (VSE) when the VSE deployment fails, select only the **VSE** check box.

- 5 Perform one of the following actions:

If...	Then...
You want to deploy the software to a single device (Windows, RHEL 5, or RHEL 6),	Enter a single IP address in the <b>IP Address</b> text box.
You want to deploy the software to a list of Windows or RHEL 6 devices,	<ol style="list-style-type: none"> <li>1 Click the plus (+) icon next to the <b>IP Addresses</b> text box.</li> <li>2 Browse to the appropriate text file with IP addresses of the devices.</li> <li>3 Click <b>OK</b>.</li> </ol>

**Step result:** IP addresses from the text file appear in the **IP Addresses** text box.

- 6 Click **OK**.

**Step result:**

The **PowerShell** window displays the deployment status.

- 7 If the system fails, verify the reasons for failure, resolve the issues, and repeat the steps.

**Result:** The **Agent Report** window appears when all systems and tasks complete.



## Changing Logon Banners

The procedures in this section can be used to change a default logon banner to one specifically suited for your organization.

Perform [Changing Logon Banners Locally on page 39](#) for any devices that are not joined to the domain.

Perform [Changing Logon Banners Through a Domain Controller on page 40](#), then [Changing Logon Banners Locally on page 39](#) for any devices that are joined to the domain.

### Changing Logon Banners Locally

**When and where to use:** Perform this procedure to change the logon banner for a Windows-based device from the Local Security Settings window on that device.

**Procedure:**

- 1 Log on to the Windows-based device using the local Windows administrator account (the Windows administrator account set up by Motorola is “motosec” for Windows Server devices and “secmoto” for Windows Vista and Windows 7 devices).
- 2 Insert the *Windows Supplemental* CD into the DVD drive.



**Note:** If you are performing this procedure on a Windows-based device that is implemented as a virtual machine, you first need to connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental* CD. Refer to the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.


- 3 Depending on your organization’s policies, navigate to one of the following folders on the CD drive:
  - \Motorola Windows Supplemental Fullconfig\Scripts\WindowsLogonBanner
  - \Motorola Windows Supplemental Transconfig\Scripts\WindowsLogonBanner
- 4 Copy the following files to the C:\windows\temp location:
  - setLogonBanner-source.exe
  - setWindowsLogonBanner.vbs
  - LogonBanner.txt
- 5 Depending on your organization's policies, perform one of the following:

If...	Then...
If your organization does not require a logon banner,	Go to <a href="#">step 8</a> .
If your organization requires a logon banner,	Perform one of the following actions: <ul style="list-style-type: none"> <li>• In the C:\windows\temp folder, right-click the <b>LogonBanner.txt</b> file.</li> <li>• Click <b>Edit</b>.</li> </ul> <b>Step result:</b> The LogonBanner.txt file opens in the editor window.

- 6 In the editor, perform the following actions:
  - a) On the first line, enter: Title:
  - b) Make sure the second line contains the banner title.
  - c) On the third line, enter: Text:
  - d) Type the Message text for the logon banner.**Step example:** Example of a LogonBanner.txt file format:

```
Title:
Warning: This is a monitored computer system.
Text: Illegal and unauthorized use of this device
and any related service is strictly prohibited...
```

- 7 Save the LogonBanner.txt file and close the editor.
- 8 Open the Command Prompt and navigate to the C:\windows\temp folder.
- 9 Depending on your organization's policies, perform one of the following actions:

If...	Then...
<b>If your organization does not require a logon banner,</b>	Enter: setLogonBanner-source.exe -U <b>Step result:</b> The login banner value is set to undefined in the local policy.
<b>If your organization requires a logon banner,</b>	Enter: setLogonBanner-source.exe <b>Step result:</b> The login banner value is the text entered in the LogonBanner.txt file.  <b>Note:</b> If the User Account Control dialog box appears, click <b>Continue</b> , or type the administrator password for the account displayed then click <b>Yes</b> , depending on the prompt you see.

- 10 Close the Command Prompt window.
- 11 Restart the device.

**Post requisites:** To verify if this procedure has been performed successfully, log out and log in to the client using the valid username and password. As a result, a warning banner with the text you entered is displayed.

## Changing Logon Banners Through a Domain Controller

**When and where to use:** Perform this procedure to change logon banners by editing a Group Policy Object (GPO) on the ASTRO<sup>®</sup> 25 system domain controller.

### Procedure:

- 1 Log in to the system-level domain controller using the local administrator account or an account from the Active Directory “Domain Admins” group.  
In either case, the account set up by Motorola is “motosec”.
- 2 Depending on your organization's policies, perform one of the following:
  - If your organization requires a logon banner, navigate to the C:\Program Files\Motorola\AstroDC\AD\data folder.
  - If your organization does not require a logon banner, go to [step 6](#).
- 3 Right-click the **LogonBanner.txt** file and click **Edit**.  
**Step result:** The LogonBanner.txt file opens in the editor.
- 4 In the editor, perform the following actions:
  - a) On the first line, enter: **Title:**
  - b) Make sure the second line contains the banner title.
  - c) On the third line, enter: **Text:**
  - d) Type the Message text for the logon banner.

**Step example:** Example of a **LogonBanner.txt** file format:

```
Title:
Warning: This is a monitored computer system.
Text:
```



Illegal and unauthorized use of this device and any related service is strictly prohibited..

- 5 Save the **LogonBanner.txt** file and close the editor.

**Step result:** The editor window is closed.

- 6 From the Start menu, select **All Programs → Accessories → Windows PowerShell → Windows PowerShell**. You can also launch PowerShell by clicking the icon on the taskbar.
- 7 In the **PowerShell** window, navigate to C:\Program Files\Motorola\AstroDC\AD\scripts.
- 8 Perform one of the following actions:

If...	Then...
<b>If your organization follows the DISA/FDCC standard,</b>	Enter: <code>.\setWindowsLogonBanner.ps1 -U</code>  <b>Step result:</b> The login banner value in the BHT_ADM GPO is set to “Not Defined”.
<b>If your organization’s policy is for GPOs to define that no logon banner will display,</b>	Enter: <code>.\setWindowsLogonBanner.ps1 -D</code>  <b>Step result:</b> The login banner value is set to “Defined” and blank in the BHT_ADM GPO.
<b>If your organization’s policy is for GPOs to define that a logon banner will display, using text from LogonBanner.txt file,</b>	Enter: <code>.\setWindowsLogonBanner.ps1</code>  <b>Step result:</b> The login banner value is set to “Defined” and value is set to the text entered in the LogonBanner.txt file in the following location:  C:\Program Files\Motorola\AstroDC\AD\data

- 9 Close the **PowerShell** window.

## Removing BAR Client and Event Logging Client Software

### When and where to use:

If ASTRO® 25 system Backup and Restore (BAR) client software or the Centralized Event Logging client software was installed as part of deploying a Windows-based virtual machine, such as the MOSCAD NFM Graphical Master Computer (GMC), you will see options for these clients.

If your organization does not use these services, remove the BAR client and Centralized Event Logging client software using the standard function for removing programs from a Windows environment. For example, the GMC virtual machine is hosted on a Windows Server 2008 operating system.

For more information, see the *Backup and Restore Services* and the *Centralized Event Logging* manuals.

### Procedure:

- 1 Verify if BAR or Centralized Event Logging client software was installed. From the **Start** menu, select **All Programs → Motorola**.
- 2 If BAR or Centralized Event Logging client software is present, from the **Start** menu, select **Control Panel → Uninstall a program**.
- 3 Uninstall the BAR client:
  - a) Select **Motorola Windows Bar Client**.
  - b) Click the **Uninstall** button above the list.
  - c) Select **Motorola Common Cygwin**.
  - d) Click the **Uninstall** button above the list.
  - e) Reboot the Windows-based device.
- 4 Uninstall the Centralized Event Logging client:

- a) Select **Motorola Windows Logging Client**
- b) Click the **Uninstall** button above the list.



**Note:** The SYSLOG-NG and SNARE services continue to appear as running, but they do not function properly without the Motorola Windows Logging Client installed. These services no longer appear in the list of currently installed programs after the Windows-based device is restarted.

# Chapter

# 3

## Remote Desktop Installation and Configuration

This section provides procedures for Windows-based devices that may need remote access.

### Applying Remote Desktop Updates for Windows XP, Windows Server 2003, and Windows Vista

---

**When and where to use:** This procedure describes how to apply remote desktop updates.



**Note:** The following procedure should **not** be performed on devices operating on:

- Windows Server 2008
- Windows XP Service Pack 3 or higher
- Windows 7 Professional edition OS

#### Procedure:

- 1 Log in to the Windows-based device using the local Windows administrator account (the Windows administrator account set up by Motorola is “motosec” for Windows Server devices and “secmoto” for Windows Vista devices).
- 2 Insert the *Windows Supplemental* CD into the DVD drive.



**Note:** If you are performing this procedure on a Windows-based device that is implemented as a virtual machine, you first need to connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental* CD. Refer to the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO<sup>®</sup> 25 system.

- 3 Open the Windows command prompt.

**Step result:** The Windows command prompt appears.

- 4 Navigate to the \WIF directory on the CD/DVD drive.
- 5 Execute the following command:

```
WindowsInstallFramework.exe /e /i remote_desktop_updates.xml
```



**Note:** If the **User Account Control** dialog box appears, click **Continue**, or type the administrator password for the account displayed then click **Yes**, depending on the prompt you see.

**Step result:** An installation finished message appears.

### Using Windows Remote Desktop Connection

---

**When and where to use:** Using the Windows Remote Desktop Connection (RDC), you can connect to a terminal server or to another computer running Windows, with the proper network access and permissions. The Remote Desktop Connection software communicates over a TCP/IP network connection using Microsoft Remote Desktop Protocol (RDP). Perform this procedure to log on or log off a remote computer or server using Windows Remote Desktop Connection.



**Note:** The Windows Remote Desktop is automatically installed as part of the operating system installation.

**Procedure:**

- 1 From the list of Programs in the **Start** menu, select **Accessories → Communications → Remote Desktop Connection**.

**Step result:** The **Remote Desktop Connection** dialog box appears.

- 2 Select an available computer on the domain by clicking the drop-down arrow, and select **<Browse for more...>**.

**Step result:** A **Browse for Computers** dialog box appears with a hierarchal tree of all available network computers.



**Note:** The dialog box may not show all the computers in the network. To connect to a system, enter the Fully Qualified Domain Name (FQDN) of that system.

- 3 Click **Connect**.

**Step result:** The desktop of the remote computer appears.

- 4 Log on to the remote computer using the user name and password provided by your system administrator.

**Step result:** The Windows Remote Desktop session begins.

- 5 To log off completely from a Windows Remote Desktop session, select **Start → Log off**.



**Note:**

- The CTRL+ALT+DEL option cannot be used to log off from the remote session.
- Clicking **X** in the Remote Desktop Connection dialog box closes this dialog box and not the remote session.

## Allowing Multiple User Sessions on a Device

---

If your organization's policies allow multiple interactive user sessions on a device, you can perform the following procedures so that you can use Remote Desktop Connection to access a Windows-based device when a user is already logged on to that device.



**Important:** Leaving the maximum number of sessions at one per device improves performance because it reduces the demand that can be placed on system resources. If each user is sure to log off a device when finished with it, the setting of one session per device can be sufficient.

## Changing Maximum Connections for Each Device in a Domain

**When and where to use:** If your organization's policies allow multiple user sessions on each device in a domain, you can perform this procedure to change the maximum number of Terminal Services (Remote Desktop Services) connections on each Windows-based device in a domain.

**Procedure:**

- 1 Log in to the system-level Domain Controllers using the local domain administrator account or an Active Directory account that is a member of the Domain Admins user group.

In either case, the account name set up by Motorola is “motosec”.

- 2 Navigate to the **Server Manager**.

**Step example:** Type `gpmc.msc` in the command field.

- 3 In the left pane of the **Server Manager** window, navigate to **Features → Group Policy Management**.

- 4 Expand the tree under **Group Policy Management**, as needed, to navigate to **Group Policy Objects** under the ASTRO® 25 system domain.

- 5 Depending on the Windows operating system of the device where you want to limit Remote Desktop connections, click one of the following **Group Policy Objects**:
  - **DHT\_2008\_ADM**
  - **DHT\_ADM\_Vista**
  - **DHT\_ADM** (for Windows XP)
  - **DHT\_7\_ADM** (for Windows 7)

**Step result:** Information about the selected Group Policy Object appears in the right pane. The devices that use this policy are listed on the **Scope** tab.
- 6 After confirming the Group Policy Object you want to edit, based on the devices listed on its Scope tab, right-click the **Group Policy Object** and select **Edit**.
- 7 Under **Computer Configuration**, expand each of the following:
  - a) **Policies**
  - b) **Administrative Templates**
  - c) **Windows Components**
  - d) **Remote Desktop Services**
  - e) **Remote Desktop Session Host**
- 8 Click **Connections**.
 

**Step result:** Policy settings display.
- 9 In the right pane, double-click **Limit number of connections**.
- 10 Change the value in the field next to **RD Maximum connections allowed**.
 

**Step example:**

  - If you want to allow multiple user sessions on each device in this domain, type: **999999**
  - If you want a maximum of one user session on each device, type: **1**
- 11 Click **OK**.

## Changing Maximum Connections for One Device

**When and where to use:** If your organization's policies allow multiple user sessions on a device, you can perform this procedure to change the maximum number of Terminal Services (Remote Desktop Services) connections on one Windows-based device.

### Procedure:

- 1 Log in to the Windows-based device using the local Windows administrator account.  
The local Windows administrator account set up by Motorola is “motosec” for Windows Server devices, and “secmoto” for Vista and Windows 7 devices.
- 2 Navigate to the **Microsoft Management Console** window.  
**Step example:** Type `mmc` in the command field.
- 3 Select **File** → **Add/Remove Snap-in**.
- 4 In the **Add/Remove Snap-in** window, click **Add**.
- 5 In the **Add Standalone Snap-in** window, click **Group Policy Object Editor**.
- 6 Click **Add**.
- 7 In the **Select Group Policy Object** window, click **Finish**.
- 8 In the **Add Standalone Snap-in** window, click **Close**.
- 9 In the **Add/Remove Snap-in** window, click **OK**.
- 10 In the left pane of the **Microsoft Management Console** window, expand each of the following:
  - a) **Local Computer Policy**
  - b) **Computer Configuration**
  - c) **Administrative Templates**

d) **Windows Components**

11 Perform the following actions:

a) Select **Terminal Services**.

For Windows Server 2008-based devices, expand **Remote Desktop Services**.

b) Expand **Remote Desktop Session Host**.

c) Select **Connections**.

12 In the details pane, double-click **Limit number of connections**.

**Step result:** A dialog box opens for editing the number of connections.

13 Select **Enabled**.

14 Change the value of maximum connections allowed.

**Step example:**

- If you want to allow multiple user sessions on this device, type: 999999
- If you want a maximum of one user session on this device, type: 1

15 Click **OK**.

**Step result:** The dialog box closes.

16 To save a console with these settings, from the **File** menu of the **Microsoft Management Console** window, select **Save**.

## NetMeeting on Windows Server 2003 and Windows XP SP1-2

---

In an ASTRO<sup>®</sup> 25 system, a service technician and another user can share a console in the VMware vSphere Client application so that they both can see what the other is doing, on any virtual machine in the Radio Network Infrastructure (RNI), and any RNI device that is accessible from a virtual machine. NetMeeting is not required for this purpose, and is not available on Windows Server 2008 devices and Windows 7-based devices.



**Note:** For instructions on using the vSphere Client environment, see the ASTRO<sup>®</sup> 25 system *Virtual Management Server Software* manual, and the vSphere Client online help.

NetMeeting is also **not** required for transferring files for service purposes in an ASTRO<sup>®</sup> 25 system. Remote Desktop Connection and other methods can be used, within the security restrictions of the system, which are outlined in the ASTRO<sup>®</sup> 25 system *Service Access Architecture* manual and the *Information Assurance Features Overview* manual.

For devices where NetMeeting is available, if you want to use it for sharing files, your organization's policies may require that you perform [Starting NetMeeting on Windows Server 2003 and Windows XP SP1-2 on page 46](#) to start NetMeeting in a way that enables this NetMeeting capability for service purposes, then disables it after you end the NetMeeting session.

## Starting NetMeeting on Windows Server 2003 and Windows XP SP1-2

**When and where to use:** The following procedure should **not** be performed on devices operating on:

- Windows Server 2008
- Windows XP Service Pack 3 or higher
- Windows Vista Business edition OS

However, the user can start NetMeeting on Vista Business edition OS by double-clicking **conf.exe** in the `\ProgramFiles\Netmeeting\` directory.

- Windows 7 Professional edition OS

**Procedure:**

1 Insert the *Windows Supplemental* CD into the DVD drive.



**Note:** If you are performing this procedure on a Windows-based device that is implemented as a virtual machine, you first need to connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental CD*. Refer to the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.

- 2 Navigate to the \Remote Desktop\bin\ directory on the CD.
- 3 Select the **AHT-Remote-Desktop.bat** file.
- 4 Copy this file onto the desktop and double-click it.

**Step result:** A pop-up window appears, asking to complete information for NetMeeting.

- 5 Enter the required information and click **Next**.
- 6 Click **Next**.

**Step result:** The wizard helps you tune your audio settings.

- 7 Close all other programs that play sound, or record sound, and click **Next** to continue.
- 8 Click **Next**.



**Note:** Make sure that your speaker or headphones are connected and that playback volume is acceptable.

- 9 To adjust the playback volume, use the slider bar. Click the test button to hear a sample.
- 10 Click **Next** → **Finish**.
- 11 Select **Local Area Network**.
- 12 Click **Next**.
- 13 Click **Next** → **Finish**.





# Chapter 4

## CENTRACOM Gold Elite Supplemental Configuration

After you complete the procedures in the *CENTRACOM Gold Series Installation* (68P81097E45) manual, execute the procedures in *CENTRACOM Gold Elite Operator Position Supplemental Process on page 49* and *ADM/CDM Server Supplemental Process on page 50*.

Supplemental configuration procedures that are common to all Windows-based devices should be completed prior to performing these additional procedures specific to CENTRACOM Gold Elite devices.

### CENTRACOM Gold Elite Operator Position Supplemental Process

---

**When and where to use:** Perform this process to configure centralized authentication and set permissions for a Gold Elite Operator Position (dispatch console) in an ASTRO® 25 system.

**Process:**

- 1 Join the Gold Elite Dispatch Console to the Active Directory domain managed by the ASTRO® 25 system Domain Controllers, as follows:
  - 1 Make sure the computer hostname of each Gold Elite Dispatch Console is unique in the Active Directory domain managed by the ASTRO® 25 system domain controllers. See the procedures for checking hostname uniqueness and updating system properties in the *Authentication Services* manual.



**Note:**

If you needed to change the hostname of the Gold Elite Dispatch Console so that it is unique in Active Directory, make a corresponding change to the **Network Hostname** field of the **Elite Operator Position** record in the CDM Application on the ADM/CDM server. Be sure to save the change to the CDM database. For instructions, refer to the most recent version of the *CENTRACOM Console Database Managers (CDM) User's Guide*.

If the Gold Elite Dispatch Console (operator position) was still a member of the legacy ADM/CDM Active Directory domain when changing the hostname, change the membership to **WORKGROUP** at the same time the hostname is changed. Then, authenticate this change using a Local Administrator account.

- 2 Configure DNS settings on the Gold Elite Dispatch Console. For instructions, refer to the steps for configuring Network Settings, for the appropriate operating system, in the most recent version of the *CENTRACOM Gold Series PC Software Installation Guide*. Use the DNS server IP addresses and DNS suffixes from the most recent ASTRO® 25 system configuration documentation prepared for your organization by Motorola.
- 3 Join the Gold Elite Dispatch Console to the domain managed by the ASTRO® 25 system Domain Controllers. See *Joining and Rejoining a Windows-Based Device to an Active Directory Domain with a Script on page 29*.
- 2 Set permissions for the CENTRACOM folder on the dispatch console. Refer to one of the following, depending on the dispatch console's operating system:
  - *Setting Permissions for CENTRACOM Gold Folder for Windows Vista on page 51*
  - *Setting Permissions for CENTRACOM Gold Folder for Windows XP and Windows Server 2003 on page 50*
- 3 Set permissions for CENTRACOM sharing. Refer to one of the following, depending on the dispatch console's operating system:

- [Setting Permissions for CENTRACOM Gold Sharing for Windows Vista, Windows Server 2008, and Windows 7 on page 52](#)
  - [Setting Permissions for CENTRACOM Gold Sharing for Windows XP and Windows Server 2003 on page 52](#)
- 4 Install and configure the anti-malware client application on the dispatch console, as follows:
- a) Deploy McAfee Anti-Malware Client from the Core Security Management Server to the dispatch console. See [CSMS – Deploying the McAfee Client Software to Anti-Malware Clients in RNI on page 37](#).
  - b) Perform supplemental configuration of the Anti-Malware Client. See [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#).

## ADM/CDM Server Supplemental Process

---

**When and where to use:** Perform this process to configure centralized authentication and set permissions for an ADM/CDM server in an ASTRO® 25 system.

**Process:**

- 1 Join the ADM/CDM server to the Active Directory domain managed by the ASTRO® 25 system Domain Controllers, as follows:
  - a) For ADM/CDM servers, make sure that Active Directory was uninstalled from the ADM/CDM server. See the procedure for the appropriate operating system (Windows Server 2008 or Windows Server 2003) in the most recent version of the *CENTRACOM Gold Series PC Software Installation Guide*.
  - b) Configure DNS settings on the ADM/CDM server. For instructions, refer to the steps for configuring Network Settings, for the appropriate operating system, in the most recent version of the *CENTRACOM Gold Series PC Software Installation Guide*. Use the DNS server IP addresses and DNS suffixes from the most recent ASTRO® 25 system configuration documentation prepared for your organization by Motorola.
  - c) Join the ADM/CDM server to the domain managed by the ASTRO® 25 system Domain Controllers. See [Joining and Rejoining a Windows-Based Device to an Active Directory Domain with a Script on page 29](#).
- 2 Set permissions for the CENTRACOM folder on the ADM/CDM server. Refer to one of the following, depending on the ADM/CDM server's operating system:
  - [Setting Permissions for CENTRACOM Gold Folder for Windows Vista on page 51](#)
  - [Setting Permissions for CENTRACOM Gold Folder for Windows XP and Windows Server 2003 on page 50](#)
- 3 Set permissions for CENTRACOM sharing. Refer to one of the following, depending on the ADM/CDM server's operating system:
  - [Setting Permissions for CENTRACOM Gold Sharing for Windows Vista, Windows Server 2008, and Windows 7 on page 52](#)
  - [Setting Permissions for CENTRACOM Gold Sharing for Windows XP and Windows Server 2003 on page 52](#)
- 4 Install and configure the anti-malware client application on the ADM/CDM server, as follows:
  - a) Deploy McAfee Anti-Malware Client from the Core Security Management Server to the ADM/CDM server. See [CSMS – Deploying the McAfee Client Software to Anti-Malware Clients in RNI on page 37](#).
  - b) Perform supplemental configuration of the Anti-Malware Client. See [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#).

## Setting Permissions for CENTRACOM Gold Folder for Windows XP and Windows Server 2003

---

**When and where to use:** This procedure describes how to set permissions for the \CENTRACOM Gold\ folder for devices operating on Windows XP or Windows Server 2003.



**Note:** This procedure may be omitted if the installed CENTRACOM Gold Series version is R09.00.03 or later. These versions automate the folder permissions as part of the CENTRACOM installation.

To determine if you need to perform this procedure:

- 1 Navigate to the **Control Panel**.
- 2 Open the utility for adding and removing programs (in Vista, **Programs and Features**).
- 3 If the version number does **not** display next to **CENTRACOM Gold Series** in the list of programs, select **CENTRACOM Gold Series** and click **Change**. The version displays in the window title.

**Procedure:**

- 1 Navigate to C:\Program Files\CENTRACOM Gold\
- 2 Right-click the \CENTRACOM Gold\ directory and select **Properties** from the menu.
- 3 In the **CENTRACOM Gold Properties** window, click the **Security** tab.
- 4 In the **Group or user names** section, highlight **Everyone** and click **Remove**.
- 5 Click **Add**.
- 6 In the **Select Users, Computers or Groups** window, type `Authenticated Users` and click **OK**.

**Step result:** The **Authenticated Users** entry appears in the **Group or user names** section.

- 7 Highlight the **Authenticated Users** entry, select the **Full Control** check box in the **Allow** column, and click **OK**.

## Setting Permissions for CENTRACOM Gold Folder for Windows Vista

---

**When and where to use:** This procedure describes how to set permissions for the \CENTRACOM Gold\ folder for dispatch consoles operating on Windows Vista Business Edition.



**Note:** This procedure may be omitted if the installed CENTRACOM Gold Series version is R09.00.03 or later. These versions automate the folder permissions as part of the CENTRACOM installation.

To determine if you need to perform this procedure:

- 1 Navigate to the **Control Panel**.
- 2 Open the utility for adding and removing programs (in Vista, **Programs and Features**).
- 3 If the version number does not display next to CENTRACOM Gold Series in the list of programs, select **CENTRACOM Gold Series**, and click **Change**. The version displays in the window title.

**Procedure:**

- 1 Navigate to: C:\Program Files\CENTRACOM Gold\.
- 2 Right-click the \CENTRACOM Gold\ directory and select **Properties** from the menu.
- 3 In the **CENTRACOM Gold Properties** window, click the **Security** tab.
- 4 Click **Edit**.
- 5 In the **Permissions for CENTRACOM Gold** window, click **Add** to open the **Select Users or Groups** window.

**Step result:** The **Select Users or Groups** window appears.

- 6 In the bottom window, type `Authenticated Users` and click **OK**.

**Step result:** The **Authenticated Users** entry appears in the **Group or user names** section.

- 7 Highlight the **Authenticated Users** entry, select the **Full Control** check box in the **Allow** column and click **OK**.

## Setting Permissions for CENTRACOM Gold Sharing for Windows XP and Windows Server 2003

---

**When and where to use:** This procedure describes how to set permissions for CENTRACOM Gold sharing for devices operating on Windows XP or Windows Server 2003.

**Procedure:**

- 1 Navigate to `C:\Program Files\CENTRACOM Gold\`
- 2 Right-click the `\CENTRACOM Gold\` directory and select **Properties** from the menu.
- 3 In the **CENTRACOM Gold Properties** window, click the **Sharing** tab.
- 4 Click **Permissions**.

**Step result:** The **Permissions for CENTRACOM Gold** window appears.

- 5 In the **Group or user names** section, highlight **Everyone** and click **Remove**.
- 6 Click **Add**.
- 7 In the **Select Users, Computers or Groups** window, type `Authenticated Users` and click **OK**.

**Step result:** The **Authenticated Users** entry appears in the **Group or user names** section.

- 8 Highlight the **Authenticated Users** entry, select the **Full Control** check box in the **Allow** column, and click **OK**.

## Setting Permissions for CENTRACOM Gold Sharing for Windows Vista, Windows Server 2008, and Windows 7

---

**When and where to use:** This procedure describes how to set permissions for CENTRACOM Gold sharing for devices operating on Windows Vista Business Edition, Windows Server 2008, or Windows 7.

**Procedure:**

- 1 Navigate to one of the following, depending on the type of the operating system:
  - `C:\Program Files\CENTRACOM Gold\` for Windows Vista
  - `C:\Program Files (x86)\CENTRACOM Gold` for Windows Server 2008 and Windows 7
- 2 Right-click the `\CENTRACOM Gold\` directory and select **Properties** from the menu.
- 3 In the **CENTRACOM Gold Properties** window, click the **Sharing** tab.
- 4 Click **Advanced Sharing**.
- 5 In the **Advanced Sharing** window, select the check box next to **Share this folder**.
- 6 Click **Permissions**.

**Step result:** The **Permissions for CENTRACOM Gold** window appears.

- 7 In the **Group or user names** section, highlight **Everyone** and click **Remove**.
- 8 Click **Add**.

**Step result:** The **Select Users or Groups** window appears.

- 9 In the bottom window, type `Authenticated Users` and click **OK**.

**Step result:** The **Authenticated Users** entry appears in the **Group or user names** section.

- 10 Highlight **Authenticated Users**, select the **Full Control** check box in the **Allow** column, and click **OK**.

# Chapter

# 5

## Windows Supplemental Configuration Troubleshooting

This chapter provides information about the configuration settings applied by the procedure [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#).

### Windows Supplemental Configuration – Types of Settings Applied

---

If you are troubleshooting problems with a Windows-based device in an ASTRO<sup>®</sup> 25 system, you can view types of supplemental configuration settings that were applied to that device.

The following are examples of settings applied by the [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#) procedure. The actual settings applied depend on the device selected during the procedure:

- Applies OS-specific settings (if a device supports more than one operating system, the Device Specific Settings function on the *Windows Supplemental* CD automatically detects the operating system and applies the appropriate settings)
- Applies application-specific settings
- Configures Microsoft-installed applications, as follows, if your organization's policies require it:
  - Disables Media Player (Windows XP-based devices and Windows Server 2003 devices only)
  - Removes games, MSN and ASPNET access (Windows XP-based devices only)
  - Disables Windows Messenger (Windows XP-based devices only)

The supplemental configuration settings of Microsoft-installed applications are summarized for each Windows-based device in a .txt file in one of the following directories on the *Windows Supplemental* CD, depending on your organization's policies:

- \Motorola Windows Supplemental Fullconfig\bin
- \Motorola Windows Supplemental Transconfig\bin

Each row of the .txt file includes types of information from the following table.

**Table 4: Windows Supplemental Configuration – Format of Motorola's List of Settings Automatically Applied**

Identifier	If configuration of Microsoft-installed applications is needed (.NET, Media Player, Games, MSN, ASPNET, Messenger)	If OS-specific settings are needed:	If device-specific settings are needed:
<device name or names>;	\<common setting name>;\<common setting name>;etc.	\<OS name>;	\<device name>;

---

If the Windows Logging Client check box or the Windows BAR Client check box were selected during [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#), this configuration is displayed in the last two rows of the .txt file.

If more than one device name appears at the beginning of a row in the .txt file, this indicates applications that reside on the same Windows-based device, as specified by the user during [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#).



**Important:** The combinations available for selection during [Applying Device-Specific Settings Using the Windows Supplemental CD on page 33](#) are the only combinations of applications that have been designed and tested by Motorola for cohabitation on the same Windows-based device in ASTRO<sup>®</sup> 25 systems.